AMENDMENTS TO THE CLAIMS

Claims 1-20 (Canceled without prejudice).

Please add Claims 21-70 as follows:

21. (New) A method for automated self-repair of a computer from a software corruption, a virus infection, and a malicious software attack at anytime during operation of the computer including at startup and anytime after startup during use of the computer, the computer being of the type having a first storage that stores executable computer program instructions and a processor coupleable to the first storage, to a first random access memory, and to a first BIOS memory storing a basic input-output system (BIOS), the method comprising:

in a second storage disposed within the housing of the computer: (i) storing a master template and (ii) a repair procedure that are completely isolated and protected from alteration by viral infection and malicious code from untrusted sources, and (iii) allocating storage for storing a user modified data or program, the user data allocated space, the master template, and the repair procedure being stored on logically different and separately addressable and isolated storage from each other and from the first storage, the second storage not capable of being exposed to the an untrusted data or program source;

selectively operating the computer in a normal mode and a repair mode wherein:

(a) in the normal mode, the first storage is physically present within the housing of the computer and able to support read and write operations, and the second storage is physically present within the housing of the computer but logically hidden and unable to support a write operation communication from the first storage, the first processor, the first random access memory, or the first BIOS memory; and

(b) in the repair mode, the first storage is physically present in the computer and able to support read and write operations, and the second storage is physically present in the computer and logically visible and able to have only predetermined communication controlled by the repair procedure with the first storage, the predetermined communication being permitted only through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free;

switching the computer operation from the normal mode to the repair mode in response to a repair start signal;

automatically and without user intervention repairing the first storage to a known operational state that supports normal mode operation including generating the executable computer program instructions on the first storage using the repair procedure to copy at least a portion of the master template to the first storage through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free; and

after completing the repairing, then automatically returning to normal mode operation.

22. (New) A method as in claim 21, wherein the trusted processor and memory are the first processor, first random access memory, and first BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage.

23. (New) A method as in claim 21, wherein the trusted processor and memory are a second processor, a second random access memory, and a second BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage.

24. (New) A method as in claim 21, wherein the system further provides an integrated second computing system operating concurrently with the computing system and having a second processor and a second random access memory coupled with the second processor, and the method further comprising:

executing a second computing process concurrent with a first computing process involving the first processor, the first random access memory, and the first storage;

the second computing process utilizing at least one of: (i) the first storage in a shared configuration, (ii) a functionally mirrored version of at least a portion of the first storage, and (iii) a quarantined storage different from the first storage;

the second computer process monitoring activity in the first process and detecting a problem event based on the monitoring; and

in response to detecting the problem event, using the second computing system to repair the problem event, the using of the second computing system including clearing the contents or the first processor and first random access memory, and another process selected from: (i) switching from the first computing system to second computing system to continue first computer system processing until the first computing system can be repaired; (ii) maintaining processing in the first computing system while the second computing system marks repairs to the first computing system; and (iii) combinations of (i) and (ii).

25. (New) A method as in claim 21, wherein switching the computer operation from the normal mode to the repair mode in response to a repair start signal; including: (1) if the first storage is the computer primary boot device, then altering the computer or the first storage device so that the first storage is no longer identified as the primary boot device; and (2) if the second storage is not configured as the computer primary boot device, then altering the computer or the second storage device so that the second storage is from then identified as the primary boot device.

26. (New) A method as in claim 25, wherein the automatically returning to normal mode operation includes: (i) altering the computer or the second storage device so that the second storage is not the primary boot device and is not logically visible to the computer, and (ii) altering the computer or the first storage device so that the first storage is identified as the primary boot device.

27. (New) A method as in claim 26, further comprising automatically rebooting the repaired computer from the bootable first storage using the processor and not using the second storage to the normal mode.

28. (New) A method as in claim 21 , further comprising:

generating the start repair signal from a location physically distant from the computer and conducting the repair without further user interaction.

29. (New) A method as in claim 24, further comprising operating a third computing system to control the monitoring and repair of the first computing system while the second computing system takes over first processing system operations.

30. (New) A method as in claim 21, further comprising updating and storing the updated master template so that a repaired computer system is repaired with a current updated operating system, application programs, and customized preferences and parameters, the updating and storing comprising:

performing a backup of user data;

entering the repair mode of operation;

clearing the first processor, the first random access memory, and the first computer basic input-output system (BIOS) memory, and the first storage so that no virus or malicious code remains so that they are trusted sources and cannot contaminate the master templates;

repairing the first storage by writing original master template from the second storage to the first storage;

updating or adding to any of the operating system and application programs on the first storage;

generating a new master template from the content of the first storage and the original master template;

storing the updated master template over the original master template;

optionally restoring user data not part of the master template to the first storage; and

exiting the repair mode and entering the normal mode.

31. (New) A method as in claim 30, further comprising maintaining a back-up of predetermined data types for repairing the computer without loss of the data, the backup including:

maintaining a user storage in logical isolation from the master template and the repair procedure;

storing backup data in the user storage;

the storing being conducted in a back-up mode of operation using a backup procedure stored on the second storage; and

the backup procedure including a backup application program that executes under an alternate operating system different than the operating system booting and executing from the first storage and not capable of executing instructions that may be concealed within the stored data, and

the backup data being securely stored and inaccessible to the user except during a repair mode operation.

32. (New) A method as in claim 31, further including restoring user data to the first storage, wherein the stored backup data is restored to the first storage by the repair procedure and cannot execute instructions that may be concealed within the stored data.

33. (New) A method as in claim 21, further comprising continuously or intermittently monitoring the computer for the repair start signal to initiate operation in the repair mode.

34. (New) A method as in claim 21, wherein the executable computer program instructions stored on the first storage include an operating system for the computer and application programs that execute under the operating system within the processor.

35. (New) A method as in claim 21, wherein:

the stored master template including information sufficient to create the executable computer program instructions on the first storage;

the stored repair procedure includes a repair operating system and a repair application program executing under the repair operating system; and

the repair operating system is a different operating system than an operating system stored in the master template or an operating system for operating the computer in the normal mode and stored on the first storage.

36. (New) A method as in claim 21, further including storing a backup procedure for copying data from the first storage to the second storage.

37. (New) A method as in claim 21, wherein the repair procedure is stored on a first partition of a hard disk drive, the master template is stored on a second partition of a hard disk drive, and the user data is stored on a third partition of a hard disk drive.

38. (New) A method as in claim 21, wherein in the repair mode, the predetermined communication controlled by the repair procedure is limited to copying operation communications.

39. (New) A method as in claim 21, wherein in the repair mode, the predetermined communication further include a first storage formatting operation that clears all data from the first storage.

40. (New) A method as in claim 21, wherein in the repair mode, drivers for supporting peripheral devices and other components than the first storage, the second storage, and the processor are not loaded so that recognition and operation of the peripheral devices and other components is prevented in the repair mode.

41. (New) A method as in claim 21, wherein drivers for communicating outside a physical box housing the computer are not loaded so that external communication is prevented during the repair mode and the second storage is isolated from entities external to the computer box.

42. (New) A method as in claim 21, wherein the altering of the computer or the first storage device so that the first storage is not the primary boot device includes altering the computer or the first storage device so that the first storage is not a bootable device.

43. (New) A method as in claim 21, wherein the first storage includes a hard disk drive storage and the altering of the computer or the first storage device so that the first storage is not the primary boot device includes setting the hard disk drive address to identify that the hard disk drive first storage is not the primary boot device.

44. (New) A method as in claim 21, wherein the first storage includes an IDE hard disk drive storage and the altering of the computer or the first storage device so that the first storage is not the primary boot device includes setting the hard disk drive IDE drive bus address to address different than ID=0 to identify that the hard disk drive first storage is not the primary boot device.

45. (New) A method as in claim 21, wherein the altering of the computer or the first storage device so that the first storage is not the primary boot device includes altering a BIOS of the computer so that so that the first storage is not identified as a bootable device.

46. (New) A method as in claim 21, wherein the altering the computer or the second storage device so that the second storage is the primary boot device further comprises maintaining the second storage in a powered down state until the computer or first storage device are configured so that the first storage is not the primary boot device and the computer or the second storage device are configured as the primary boot device.

47. (New) A method as in claim 21, wherein the second storage includes a second IDE hard disk drive and the altering the computer or the second storage device so that the second storage is the primary boot device further comprises altering the IDE hard disk drive second storage so that the IDE disk drive is set at an drive bus address ID=0.

48. (New) A method as in claim 21, wherein the second storage comprises a plurality of logical or physical devices and the logical or physical device storing the repair procedure is altered to be set as the primary boot device independent of the bootable status of other of the logical or physical devices.

49. (New) A method as in claim 21, wherein the computer automatically and without user intervention repairing further includes: repairing the processor to a known predetermined processor operational state that supports normal mode operation by clearing the processor before resetting it to an error and virus free processor operational state; and repairing a BIOS or CMOS to a known predetermined BIOS or CMOS operational state that supports normal mode operation by clearing the BIOS or CMOS before resetting it to an error and virus free BIOS or CMOS operational state.

50. (New) A method as in claim 21, wherein:

repairing the first storage to a know operational state further comprises regenerating the executable computer program instructions on the first storage; and

regenerating the executable computer program instructions on the first storage comprises one of: (a) copying at least a portion of the master template to the first storage, and installing the executable computer program instructions onto the first storage using the processor to execute the repair procedure operating on the master template as data on the second storage.

51. (New) A method as in claim 21, wherein the repair procedure includes an operating system and application program that are limited to operations that generate the executable computer program instructions on the first storage but cannot execute instructions included in the master template or the user data.

52. (New) A method as in claim 21, wherein the master template includes an operating system and the repair procedure operating system is a different operating system than an operating system of the master template.

53. (New) A method as in claim 51, wherein the limited to operations are selected from the set of operations consisting of formatting the first storage, copying bits from the second storage to the first storage.

54. (New) A method as in claim 21, wherein the signal to start operation in the repair mode is generated by a switch exposed on an external surface of the computer.

55. (New) A method as in claim 21, wherein the switch exposed on an external surface of the computer is dedicated to initiating operating in the repair mode and different from the computer power switch, computer reset switch, peripheral device operating switch, mouse button, or keyboard keys.

56. (New) A method as in claim 21, further comprising storing backup data in the user storage is performed in response to a user request or predetermined policy, and predetermined policy is a policy selected from the group of policies consisting of a periodic timed back-up, a scheduled time-of day back-up, and a user requested backup.

57. (New) A method as in claim 56, wherein the back-up is performed by changing from the normal mode to the repair mode to provide isolation during the backup and then changing back to the normal mode for continued operation.

58. (New) A method as in claim 56, wherein the user data is selected from the set of data consisting of: at least one of a user data, a computer system or program preference or customization, an operating system or application program component or upgrade, or another user or system modification.

59. (New) A method as in claim 58, further comprising quarantining a data item in an isolated storage where any executable content of the data item cannot be executed.

60. (New) A method as in claim 59, wherein the data item is an email or an email attachment.

61. (New) A method as in claim 21, wherein the repair mode procedure, including the repair mode operating system and the repair application program are executed in a second processor different from the first processor.

62. (New) A method as in claim 21, wherein the computer is booted using a second BIOS or CMOS basic input-output system different from the BIOS or CMOS used to boot the computer from the first storage and the first processor.

63. (New) A computer that can self-repair from a software corruption, a virus infection, and a malicious software attack at anytime during operation of the computer including at startup and anytime after startup during use of the computer, comprising:

a first storage disposed within the computer box and adapted to store executable computer program instructions;

a first processor coupleable to the first storage, to a first random access memory, and to a first BIOS memory storing a basic input-output system (BIOS), for executing the stored executable computer program instructions;

a second storage disposed within the computer box and adapted to store (i) a master template and (ii) a repair procedure that are completely isolated and protected from alteration by viral infection and malicious code from untrusted sources, and (iii) allocating storage for storing a user modified data or program, the user data allocated space, the master template, and the repair procedure being stored on logically different and separately addressable and isolated storage from each other and from the first storage, the second storage not capable of being exposed to the an untrusted data or program source;

the computer being configurable to selectively operate in a normal mode and a repair mode wherein:

(a) in the normal mode, the first storage is physically present within the housing of the computer and able to support read and write operations, and the second storage is physically present within the housing of the computer but logically hidden and unable to support a write operation communication from the first storage, the first processor, the first random access memory, or the first BIOS memory; and

(b) in the repair mode, the first storage is physically present in the computer and able to support read and write operations, and the second storage is physically present in the computer and logically visible and able to have only predetermined communication controlled by the repair procedure with the first storage, the predetermined communication being permitted only through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free;

first switch logic for automatically switching the computer operation from the normal mode to the repair mode in response to a repair start signal;

repair means for automatically and without user intervention repairing the first storage to a known operational state that supports normal mode operation; including means for generating the

executable computer program instructions on the first storage using the repair procedure to copy at least a portion of the master template to the first storage through a trusted processor and memory executing a repair procedure that are known to be virus and malicious code free; and

second switch logic for automatically preparing the computer to resume normal mode operation after completing the repairing.

64. A computer of the type having a processor, a random access memory coupled to the processor, and a first storage coupled for communication with the processor, the computer characterized in that:

the computer may self-repair from a software corruption, a virus infection, and a malicious software attack at anytime during operation of the computer including at startup and anytime after startup during use of the computer by automatically and without user intervention repairing the first storage using a trusted processor and memory state;

a master template and a computer repair procedure are stored as separately addressable logical volumes in storage that is physically present within the computer at the time a failure occurs but completely isolated and protected from alteration before use and during use to repair the computer by viral infection and malicious code from any source having a unknown or uncertain content within the computer or external to the computer, including being protected from the processor, processor coupled random access memory, and the first storage;

the computer is selectively operable in at least a normal mode and a repair mode, the mode of operation being selectable at least by a user pressing a single repair mode switch operable from an external service of the computer, wherein:

in the normal mode, the second storage is logically hidden from the computer system and not available as a bootable device so that no access is permitted to the second storage and optionally not electronically coupled for communication with the processor being one of (i) powered off, (ii) not coupled to a computer communication bus, or both powered off and not coupled to a computer communication bus; and

in the repair mode, the second storage is logically visible to the computer system only through an operating system component of the trusted repair procedure and available as a readable/writable and bootable device only after the processor and the random access memory coupled to the processor have been cleared of all unknown or uncertain content from operation in the normal mode and all communication with external entities has been disabled, the trusted repair procedure preventing execution of any content stored on the first storage while in the repair mode.

65. (New) A computer as in claim 63, wherein the trusted processor and memory are the first processor, first random access memory, and first BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage.

66. (New) A computer as in claim 63, wherein the trusted processor and memory are a second processor, a second random access memory, and a second BIOS memory that have been cleared of any executable virus or malicious code by the repair procedure prior to permitting any communication with the second storage.

67. (New) A computer as in claim 63, wherein the system further provides an integrated second computing system operating concurrently with the computing system and having a second processor and a second random access memory coupled with the second processor, and wherein:

the second computing process executes concurrent with a first computing process involving the first processor, the first random access memory, and the first storage;

the second computing process utilizing at least one of: (i) the first storage in a shared configuration, (ii) a functionally mirrored version of at least a portion of the first storage, and (iii) a quarantined storage different from the first storage;

the second computer process monitoring activity in the first process and detecting a problem event based on the monitoring; and

in response to detecting the problem event, using the second computing system to repair the problem event, the using of the second computing system including clearing the contents or the first processor and first random access memory, and another process selected from: (i) switching from the first computing system to second computing system to continue first computer system processing until the first computing system can be repaired; (ii) maintaining processing in the first computing system while the second computing system marks repairs to the first computing system; and (iii) combinations of (i) and (ii).

68. (New) A computer as in claim 63, wherein changing the computer operation from the normal mode to the repair mode in response to a repair start signal; including switching logic that: (1) if the first storage is the computer primary boot device, then altering the computer or the first storage device so that the first storage is no longer identified as the primary boot device; and (2) if the second storage is not configured as the computer primary boot device, then altering the computer or the second storage device so that the second storage is from then identified as the primary boot device.

69. (New) A computer as in claim 68, wherein the automatically returning to normal mode operation includes: (i) altering the computer or the second storage device so that the second storage is not the primary boot device and is not logically visible to the computer, and (ii) altering the computer or the first storage device so that the first storage is identified as the primary boot device.

70. (New) A computer as in claim 69, further comprising:

means for updating and storing the updated master template so that a repaired computer system is repaired with a current updated operating system, application programs, and customized preferences and parameters, the updating and storing comprising:

means for performing a backup of user data;

means for entering the repair mode of operation;

means for clearing the first processor, the first random access memory, and the first computer basic input-output system (BIOS) memory, and the first storage so that no virus or malicious code remains so that they are trusted sources and cannot contaminate the master templates;

means for repairing the first storage by writing original master template from the second storage to the first storage;

means for updating or adding to any of the operating system and application programs on the first storage;

means for generating a new master template from the content of the first storage and the original master template;

means for storing the updated master template over the original master template;

means for optionally restoring user data not part of the master template to the first storage; and

means for exiting the repair mode and entering the normal mode; and

means for maintaining a back-up of predetermined data types for repairing the computer without loss of the data, the backup including:

means for maintaining a user storage in logical isolation from the master template and the repair procedure;

means for storing backup data in the user storage;

the means for storing being conducted in a back-up mode of operation using a backup procedure stored on the second storage; and

the backup procedure including a backup application program that executes under an alternate operating system different than the operating system booting and executing from the first storage and not capable of executing instructions that may be concealed within the stored data, and

the backup data being securely stored and inaccessible to the user except during a repair mode operation.